06-09-06

AF ZFW

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/750,255
Filing Date: December 28, 2000
Appellants: SHRADER ET AL.

Primary Examiner:
Thomas M. Ho

REPLY BRIEF

"Express Mail" Mailing Label Number EQ 708327250 US
Date of Deposit: June 8, 2006
I hereby certify that this paper or fee is being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, P. O. Box 1450, Alexandria, Virginia 22313-1450

Darcell Walker, Reg. No. 34,945

This reply brief is in response to the Examiner's Answer filed March 8, 2006 responding to the Appellants' Appeal April 21, 20005.

Response to Examiner's Arguments in Reply Brief

The rejections the claims are novelty rejections based on 35 U.S.C. 102(e) citing Sudia et al. (U.S. Patent 6,209,091) and 35 U.S.C. 102(b) citing Internet Explorer 3 for Windows for Dummies, Doug Lowe, IDG Books, 1996, pages 139-153. For rejections to be supported under both sections 35 U.S.C. 102(e) and 35 U.S.C. 102(b), the cited reference must disclose each element of a rejected claim. Applicants initially asserted that the cited references do not describe every element of the claims in the invention. In view of the Examiner's response, Applicants still assert that the cited references do not disclose each element of the claimed invention.

The Applicants' present invention allows multiple stops in a complete transmission and retains the history and integrity of the stops, as well as any modifications made by the stop point along the way. This invention allows any number of entities to participate in the sealed transaction, wherein each entity can add to the transaction, the complete transaction is protected from unintended recipients, and authentication and integrity is ensured with each entity. During the transmission, an entity may receive the transmitted message. The entity may add information or modify information in the message. The changes would be recorded in a data structure called a SignedData object. Each new entity that receives the message during the transmission may add a SignedData object to the transmitted. Through the SignedData objects, at the end of the transmission, there is a complete record of the events that occurred during the transmission of that message. In this method, the authenticity and integrity of the transaction is preserved.

Sudia describes a multi-step signing system and method that uses multiple signing devices to affix a single signature, which can be verified using a single public verification key. Each signing device possesses a share of the signature key and affixes a partial signature in response to authorization from a plurality of authorizing agents. In a serial embodiment, after a first partial signature has been affixed, a second signing device

exponentiates the first partial signature. Sudia does not describe or mention that ability to record the history of a transmission that is described in the present invention.

With regard to claim 1, Sudia does not describe the step of 'determining whether a current recipient entity is the designated recipient entity'. Paragraph [0028] of the present invention states that "the Recipient has to determine if the sender already has an existing message, which means the sender was a receiver of a previous transaction 44. If the recipient does not need to forward the message to another entity 46, the message transmission ends. When the sender does have an existing message, Recipient has to decide whether to continue to send the message or is this Recipient the final destination 45." This process determines whether the recipient is the designated recipient entity. The locations in Sudia cited by the Examiner describe the process of determining whether the document should be signed. The Sudia process looks to see if all of the parts of the signature are present to determine whether to sign a message. The process of the present invention does not look to pieces of a signature to make the determination of whether the current recipient is the designated recipient.

Second, as described in claim 2, the present invention modifies the package message information by adding substantive information to the package message. Contrary to the examiner's assertion of substantive information being a new header, or partial digital signature, in the present invention, substantive information has a content component (paragraph 0028 and item 54 in Figure 4).

Third, as described in claim 3, new data objects can be added to the message. In Sudia, the new information added is a piece of the signature. In the present invention, there is an added data object in addition to the data object of the original message. This added data object could have a field with an additional message. Again, Sudia does provide for adding message content to the transmitted message.

Applicants submit that these features of the claim invention are not described in Sudia or implemented in Sudia in the manner as claimed in the present invention.

In view of the above, Applicants respectfully submit US Patent 6,209,091 (Sudia) does not anticipate Applicants' described invention. Contrary to the Examiner's statements that all elements of Applicants' claims are disclosed in the cited reference, the step of recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message is not so disclosed in Sudia. Therefore the 35 U.S.C. § 102(e) rejection of the claims should be withdrawn.

With regard to the Internet Explorer 3 for Windows for Dummies, Applicants again assert that this description does not disclose Applicants' present invention. This article describes sending and receiving messages via the Internet. The examiner cites pages 140 and 141 as locations that describe the elements of claims 1 and 10. With regard to the step in Applicants' claim 1 of: recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message, examiner asserts that Figure 11-1 on page 140 describes this step. Figure 11-1 shows a split screen on a display. **The top portion of the display shows a list of received email messages (not a history of one message).** The description of Figure 11-1 listed on page 140 is as follows:

> As Figure 11-1 shows, Microsoft Internet Mail has a similar user interface to Internet Explorer. For example, the toolbars in Internet Mail work the same way as the Internet Explorer tools. Notice that the Microsoft Internet Mail window is divided into two major sections, called panes. The top pane, called inbox is a list of all the e-mail you have received. He bottom pane shows the text of the currently selected message.

The location cited by the examiner does not describe the activity of the message transmission history-generating step of Applicants present invention. Further, the cited reference "Keeping in Touch with Microsoft Internet Mail" does not describe a method of implementing the present invention. Therefore, the reference does not provide an enabling description of Applicants' present invention.

In view of the above, Applicants respectfully submit that the article titled "Keeping in Touch with Microsoft Internet Mail" does not anticipate Applicants'

described invention. Contrary to the Examiner's statements that all elements of Applicants' claims are disclosed in the cited reference, the step of recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message is not so disclosed in this e article titled "Keeping in Touch with Microsoft Internet Mail". Therefore the 35 U.S.C. § 102(b) rejection of the claims should be withdrawn.

7. CONCLUSION

Applicants submit that all of the pending claims are in condition for allowance. Applicants further submit that the amendments as discussed with the Examiner were for the purpose of further defining the impersonator programs of the present invention. Applicants believe that no additional search should be required in view of the type of amendments Applicants made to the claims. Therefore, withdrawal of the rejections and passage to issuance is respectfully requested.

In view of the above arguments, it is respectfully urged that the rejection of the claims should not be sustained.

Respectfully Submitted,

Darcell Walker
Reg. No. 34,945
9301 Southwest Freeway, Suite 250
Houston, Texas 77074
713-772-1255
June 8, 2006

APPENDIX A

1. (Previously presented) A general communication transmission method that enables a transmitted message to span synchronous and asynchronous protocols over a computer network during one transmission comprising:

packaging a message for transmission in a data object, the message packages including information on the original message in the transmission;

sending the packaged message to a designated recipient entity;

receiving the message by a current recipient entity at a location;

recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message; and

determining whether current recipient entity is the designated recipient entity.

2. (Previously presented) The method as described in claim 1 further comprising before said designated recipient determining step, the step of modifying the packaged message information to indicate that the current recipient entity received the package message by adding substantive information to said packaged message.

3. (Original) The method as described in claim 1 wherein said message package is a data object with data fields containing the original message, signing certificate, signature bytes and signed attributes and wherein modification of the message package comprises creating a new data object that is added to the original data object, the new data object having additional information concerning the transmission.

4. (Original) The method as described in claim 1 wherein each recipient entity uses a public key and private key pair to authenticate the packaged message origin and contents.

5. (Original) The method as described in claim 4 further comprising verifying the packaged message by a recipient entity using the sending entities public key.

6. (Original) The method as described in claim 1 wherein said step of determining whether current recipient entity is the designated recipient entity comprises determining whether the packaged message received by said recipient entity has an existing message.

7. (Previously presented) A system for transmitting messages spanning synchronous and asynchronous protocols over a computer network comprising:

a network transmission mechanism that enables transmissions across synchronous and asynchronous protocols;

a data structure for containing the information message transmitted over the computer network, the data structure having multiple fields for containing various items related to the message being transmitted;

a message transmission history file containing events of each of stop a transmitted message in route to the message destination; and

encryption key pairs to ensure authenticity and integrity of the message during transmission between sender and final receiver sites.

8. (Original) The system as described in claim 7 wherein said data structure contains information comprising original message, signing certificate, signature bytes and signed attributes.

9. (Original) The system as described in claim 7 further comprising additional data structures that can be linked and thereby added to the data structure of the original message at each receipt of the message during transmission, said additional data structures containing information about the message transmission.

10. (Previously presented) A computer program product in a computer readable medium for use in transmitting messages that span synchronous and asynchronous protocols over a computer network during one transmission comprising:

instructions for packaging a message for transmission in a data object, the message packages including information on the original message in the transmission;

instructions for sending the packaged message to a designated recipient entity;

instructions for receiving the message by a current recipient entity at a location;

instructions for recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message; and

instructions for determining whether current recipient entity is the designated recipient entity.

11. (Previously presented) The computer program product as described in claim 10 further comprising before said designated recipient determining instructions, instructions for modifying the packaged message information to indicate that the current recipient entity received the package message by adding substantive information to said packaged message.

12. (Original) The computer program product as described in claim 10 wherein said message package is a data object with data fields containing the original message, signing certificate, signature bytes and signed attributes and wherein said instructions for modifying the message package comprises creating a new data object that is added to the original data object, the new data object having additional information concerning the transmission.

13. (Original) The computer program product as described in claim 10 further comprising instructions for using a public key and private key pair to authenticate the packaged message origin and contents.

14. (Original) The computer program product as described in claim 13 further comprising verifying the packaged message by a recipient entity using the sending entities public key.

15. (Original) The computer program product as described in claim 10 wherein said instructions for determining whether current recipient entity is the designated recipient entity comprises instructions for determining whether the packaged message received by said recipient entity has an existing message.

16. (Previously presented) A computer connectable to a distributed computing environment and including a mechanism for transmitting messages spanning synchronous and asynchronous protocols over a computer network comprising:

a processor;

a native operating system;

a network transmission mechanism that enables transmissions across synchronous and asynchronous protocols;

a data structure for containing the information message transmitted over the computer network, the data structure having multiple fields for containing various items related to the message being transmitted;

a means for generating and storing a history of intermediate stops that occurred during the transmission of an information package; and

encryption key pairs to ensure authenticity and integrity of the message during transmission between sender and final receiver sites.

17. (Original) The computer as described in claim 16 wherein said data structure contains information comprising original message, signing certificate, signature bytes and signed attributes.

18. (Original) The computer as described in claim 16 further comprising a means for linking additional data structures to the data structure of the original message at each receipt of the message during transmission, said additional data structures containing information about the message transmission at each receipt.